R E P U B L I Q U E F R A N Ç A I S E

PCT/FR2004/050510

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 19 NOV. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1. a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*03

REQUÊTE EN DÉLIVRANCE page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 @ W / 210502

Réservé à l'INPI

REMISE DES PIÈCES
DATE 24 OCT 2003
LIEU 54 INPI NANCY
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0312435
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 24 OCT. 2003

Vos références pour ce dossier *(facultatif)* 016916

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT
9, rue Claude Chappe
Metz Technopôle
57070 METZ

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE — **Cochez l'une des 4 cases suivantes**

Demande de brevet	☒	
Demande de certificat d'utilité	☐	
Demande divisionnaire	☐	
Demande de brevet initiale	N°	Date
ou demande de certificat d'utilité initiale	N°	Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N°	Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé et dispositif associé de génération de nombres aléatoires dans un intervalle donné.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation — Date — N°
Pays ou organisation — Date — N°
Pays ou organisation — Date — N°
☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases) ☒ **Personne morale** ☐ **Personne physique**

Nom ou dénomination sociale		GEMPLUS
Prénoms		
Forme juridique		Société Anonyme
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	Avenue du Pic de Bertagne Parc d'Activités de GEMENOS
	Code postal et ville	13420 GEMENOS
	Pays	FRANCE
Nationalité		française
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 24 OCT 2003
LIEU 54 INPI NANCY
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0312435

DB 540 W / 210502

6 MANDATAIRE *(s'il y a lieu)*		
Nom		LECLAIRE
Prénom		Jean-Louis
Cabinet ou Société		CABINET BALLOT
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	9, rue Claude Chappe Metz Technopôle
	Code postal et ville	5 7 0 7 0 METZ
	Pays	FRANCE
N° de téléphone *(facultatif)*		03.87.74.81.36
N° de télécopie *(facultatif)*		03.87.36.26.76
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☒ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		☐ Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint		☐
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		☐
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
Jean-Louis LECLAIRE - 93.4009

CABINET BALLOT
CONSEILS EN PROPRIÉTÉ INDUSTRIELLE
9, rue Claude Chappe
Technopôle Metz 2000
57070 METZ

VISA DE LA PRÉFECTURE OU DE L'INPI
Magali DEMANGE

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PROCEDE ET DISPOSITIF ASSOCIE DE GENERATION DE NOMBRES ALEATOIRES DANS UN INTERVALLE DONNE

L'invention concerne un procédé d'obtention d'un nombre aléatoire compris entre A et B à partir d'un générateur produisant des nombres aléatoires compris entre 0 et W-1, avec N la taille des nombres produits par le générateur, W-1 la valeur maximale prise par les nombres aléatoires produits, avec par exemple $W = 2^N$, et A, B des nombres entiers quelconques, inférieurs ou supérieurs au nombre W.

Une telle situation se produit par exemple dans un composant électronique adapté pour réaliser des calculs cryptographiques et comprenant un générateur de nombres aléatoires de N bits, par exemple N = 8. Les nombres aléatoires qu'il peut produire sont ainsi compris entre 0 et W-1 = 255, alors qu'il serait souhaitable de disposer de nombres aléatoires compris par exemple entre 0 et 100 ou entre 300 et 10000. A noter qu'il suffit de déterminer des nombres entre 0 et 9700 puis d'ajouter ensuite 300 au nombre obtenu pour obtenir finalement un nombre entre 300 et 10000.

Une telle situation se retrouve dans la pratique dans la plupart des applications cryptographiques, par exemple la signature DSA, la signature ou le chiffrement d'El Gamal, le développement de contremesures contre diverses attaques, etc.

Plusieurs procédés sont déjà connus pour produire des nombres aléatoires R compris entre 0 et K à partir de nombres compris entre 0 et W-1. Ces procédés sont en général mis en œuvre par des moyens logiciels utilisés

pour piloter d'une part un générateur hardware qui produit des nombres aléatoires de taille N et d'autre part des moyens de calcul réalisant notamment des opérations de multiplications, d'additions, etc.

Un premier procédé connu comprend les étapes suivantes :

a) déterminer le plus petit nombre entier p tel que $K \leq W^p - 1$,

b) produire p nombres aléatoires S_0, S_1, ..., S_{p-1} et former la variable $S = \sum_{i=0}^{p-1} S_i * W^i$

c) si S > K, alors retourner à l'étape b), sinon poser R = S

R est le nombre aléatoire recherché, compris entre 0 et K. L'équation $S = \sum_{i=0}^{p-1} S_i * W^i$ est une représentation de la variable S décomposée / recomposée dans la base (W^{p-1}, ..., W^1, W^0). On pourrait également noter $S = S_{p-1}S_{p-2}...S_1S_0$, notation couramment utilisée.

Un deuxième procédé connu comprend les étapes suivantes :

a) déterminer le plus petit nombre entier p tel que $K \leq W^p - 1$,

b) produire p nombres aléatoires S_0, S_1, ..., S_{p-1} et former la variable $T = \sum_{i=0}^{p-2} S_i * W^i$ et $S = T + S_{p-1} * W^{p-1}$

c) si S > K, poser R = T, sinon poser R = S.

Un troisième procédé connu comprend les étapes suivantes :

a) déterminer le plus petit nombre entier p tel que $K \leq W^p - 1$,

b) produire p nombres aléatoires S_0, S_1, ..., S_{p-1} et former la variable $S = \sum_{i=0}^{p-1} S_i * W^i$

c) poser R = S mod(K+1), c'est-à-dire le reste de la division entière de S par K+1, également appelé réduction modulaire de S par K+1.

Ces trois procédés peuvent être résumés par les étapes suivantes :

a) produire p nombres aléatoires S_0, S_1, ..., S_{p-1} , p étant le plus petit nombre entier tel que $K \leq W^p - 1$, et former la variable $S = \sum_{i=0}^{p-1} S_i * W^i$

b) déterminer le nombre aléatoire R à partir de la variable S.

Selon le cas, au cours de l'étape b, on obtient R à partir de S en répétant l'étape b (1er procédé), en tenant compte ou non du nombre aléatoire supplémentaire S_{p-1} (2ème procédé) ou en effectuant une réduction modulaire (3ème procédé).

A noter que, dans les trois procédés, si un nombre compris entre A et K+A est souhaité, il suffit d'ajouter A au nombre R obtenu compris entre 0 et K.

Le premier procédé a pour principal inconvénient un temps de calcul particulièrement long et surtout imprévisible : l'étape de production des p nombres aléatoires peut être répétée de nombreuses fois sans qu'il soit possible de prévoir au départ le nombre de répétitions de cette étape.

Le 2ème et le 3ème procédés ont pour principal inconvénient de produire des nombres aléatoires présentant un biais : parmi les nombres R produits dans l'intervalle [0, K],

certaines valeurs sont plus probables que d'autres. Dit autrement, les nombres R produits ne sont pas parfaitement aléatoires (distribution non uniforme). Ce biais peut avoir des conséquences importantes sur la sécurité des systèmes cryptographiques susceptibles de mettre en œuvre ces procédés. La sécurité des systèmes cryptographiques suppose en effet que les nombres aléatoires qu'ils utilisent soient uniformément distribués (ou au moins proches d'une distribution uniforme) dans l'intervalle [0, K] ou [A, K+A] souhaité.

Enfin, les trois procédés sont globalement lents parce qu'ils mettent en œuvre des opérations sur des grands nombres, de taille N (au sens nombre de bits) supérieure à la taille des circuits utilisés pour la mise en œuvre. En effet, le nombre K notamment, est quelconque et peut être supérieur à W et donc de taille supérieure à N. La variable S peut également être de grande taille. Or, la mise en œuvre d'opérations sur des grands nombres nécessite la mise en œuvre de procédés complexes et coûteux en termes de temps de calcul.

Un objet essentiel de l'invention est de proposer un procédé de construction d'un nombre aléatoire R particulièrement rapide.

Ainsi, l'invention propose un procédé cryptographique, au cours duquel on utilise un générateur de nombres aléatoires produisant des nombres aléatoires S_i de taille N fixée compris entre 0 et W-1, avec par exemple mais non nécessairement $W = 2^N$, pour produire un nombre aléatoire R compris entre 0 et une borne K prédéfinie.

Les étapes essentielles d'un procédé selon l'invention sont les suivantes :

E31 : on produit une variable aléatoire S_i comprise entre 0 et W-1,

E32 : si la variable aléatoire S_i est strictement inférieure à un coefficient K_i de la borne K dans la base W, alors le coefficient R_i de rang i du nombre aléatoire R est égal à la variable aléatoire S_i puis, pour tout rang j inférieur à i, on produit une variable aléatoire S_j entre 0 et W-1 et on pose $R_j = S_j$.

E33 : sinon, si la dite variable aléatoire est supérieure au coefficient K_i de rang i de la borne K dans la base W, alors on détermine le dit coefficient R_i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie, puis on détermine le coefficient R_{i-1} du nombre aléatoire R de rang i-1 immédiatement inférieur en répétant les étapes E31 à E33.

Ainsi, dans un procédé selon l'invention, on recherche un à un les coefficients R_i du nombre aléatoire R souhaité, en commençant par le coefficient R_{p-1} le plus significatif. Le générateur physique de nombres aléatoires utilisés produit ainsi des variables aléatoires S_i une à une, une variable à chaque itération.

De plus, le procédé est rapide car l'étape E33 est exécutée un nombre restreint de fois. En effet, dès qu'une des variables S_i produite par le générateur physique est inférieure au coefficient K_i associé de la borne K, le procédé ne nécessite plus le traitement des variables S_j de rang inférieur à i : on calcule ainsi le

plus souvent un nombre restreint de coefficients du nombre R, les plus significatifs.

Enfin, par rapport aux procédés connus, un procédé selon l'invention présente l'avantage de travailler sur des nombres de au plus N bits, N étant la taille des registres et autres circuits de calculs des dispositifs utilisés pour la mise en œuvre. Par exemple, si W est égal à 2^N, les coefficients K_i, résultant de la décomposition de K dans la base (W^{p-1}, ... W^1, W^0), sont nécessairement inférieurs à W et donc de taille au plus N bits. De même, les variables aléatoires S_i produites par le générateur physique de nombres aléatoires sont également de N bits.

En ajoutant aux étapes essentielles une étape d'initialisation et une étape de recombinaison du nombre aléatoire R, on obtient :

E1 : on décompose la borne K dans une base (W^{p-1}, W^{p-2}, ..., W^0) ($K = \sum_{i=0}^{p-1} K_i * W^i$ ou $K = K^{p-1}...K^1K^0$), i étant un indice de boucle, K_i étant un coefficient de la borne K de rang i compris entre 0 et W-1 et p étant le degré de la borne K,

E2 : on initialise à VRAI une variable booléenne f,

E3 : on réalise les opération suivantes, dans une boucle indicée par i, i étant un nombre entier variant entre p-1 et 0:

E31 : on produit une variable aléatoire S_i comprise entre 0 et W-1,

E32 : si la variable aléatoire S_i est strictement inférieure au coefficient K_i de rang i, alors on met à FAUX la variable booléenne f,

E33_1 : si la variable aléatoire S_i est strictement supérieure au coefficient K_i de rang i et si la variable booléenne f est VRAI, alors on détermine le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie,

E33_2 : sinon, on pose $R_i = S_i$

E34 : on décrémente l'indice de boucle i,

E4 : on détermine le nombre aléatoire R par recombinaison des coefficients aléatoires R_i dans la base W ($R = \sum_{i=0}^{p-1} R_i * W^i$ ou $R^{p-1}...R^1R^0$).

Concrètement, dès que la variable booléenne f est positionnée à FAUX, elle reste à cette valeur, puisqu'il n'est pas prévu de la repositionner à la valeur VRAI, sauf lors de l'initialisation E2 du procédé. L'étape E33 est exécutée uniquement si la variable f est VRAI ; ainsi, dès que la variable f est positionnée à la valeur FAUX, l'étape E33_1 n'est plus exécutée et le procédé selon l'invention se termine rapidement.

Un deuxième objectif de l'invention est de proposer un procédé de construction de nombres aléatoires dont la distribution soit uniforme ou puisse être rendue aussi proche que souhaitée d'une distribution uniforme. Cet objectif est atteint en choisissant une fonction adéquate pour la détermination du coefficient R_i à partir de la variable aléatoire S_i.

Selon un premier mode de mise en œuvre d'un procédé selon l'invention, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i (étape E33_1), on réalise les sous-étapes suivantes :

E33_11: si la variable aléatoire S_i est strictement supérieure au coefficient K_i de la borne K, alors on produit une nouvelle variable aléatoire S_i,

E33_12 : on répète l'étape E33_11 jusqu'à ce que la variable aléatoire S_i soit inférieure au coefficient K_i de la borne K, puis on égalise le coefficient R_i à la variable aléatoire S_i.

Dans un tel mode de réalisation, tous les coefficients R_i obtenus sont des nombres directement produits par le générateur hardware de nombres aléatoires, ces coefficients sont donc parfaits et le nombre R qui en résulte est également parfait. en d'autres termes, la distribution obtenue des nombres R est uniforme dans l'intervalle [0, K].

Selon un deuxième mode de mise en œuvre, au cours de l'étape E33, on choisit le coefficient R_i de rang i égal à une partie de la variable aléatoire S_i, partie inférieure au coefficient K_i. La dite partie correspondant dans un exemple à un nombre limité de bits de la variable S_i.

Selon un troisième mode de réalisation, au cours de l'étape E33, on réduit la variable aléatoire S_i modulo K_i+1, le résultat de la réduction étant le coefficient R_i cherché.

Ces deux derniers modes de réalisation sont rapides par rapport aux procédés connus, essentiellement parce qu'on travaille sur des petits nombres. Les distributions de nombres aléatoires obtenus ne sont cependant pas uniformes : le simple fait de tronquer la variable S_i ou d'effectuer une réduction modulo K_i+1 introduit

nécessairement un biais. Toutefois, ce biais est moindre par rapport aux procédés de l'art antérieur.

Par ailleurs, il est possible de réduire le biais des procédés selon les deuxième et troisième modes de réalisation proposés, comme on va le voir ci-dessous.

Dans un procédé selon l'invention tel que décrit ci-dessus, on construit un nombre aléatoire R inférieur à K à partir de variables S_i de taille N produits par un générateur physique parfaitement aléatoire. Le nombre R obtenu est biaisé, mais le biais est réduit par rapport à un procédé connu.

Pour cela, dans le deuxième mode ou le troisième mode de réalisation, on construit notamment au cours de l'étape E33_1 un coefficient $R_i \leq K_i$ à partir de variables S_i de taille N. Pour réduire le biais introduit sur le coefficient R_i, on propose de le construire en utilisant les mêmes étapes E1 à E3 que pour construire le nombre R. En quelque sorte, on "imbrique" deux procédés similaires. Ceci permet de réduire encore la taille des nombres sur lesquels on travaille, et en conséquence de réduire encore le biais sur les coefficients de R, et sur le nombre R final.

Concrètement, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i (étape E33_1), on exécute les étapes E1 à E4 en utilisant une base $(\beta^{q-1}, \ldots, \beta^0)$ comme base de calcul, β étant un nombre entier strictement inférieur à W et q étant le degré de K_i dans la base β.

L'étape E33 est ainsi décomposée en les sous-étapes suivantes :

E33_41 : on décompose le coefficient K_i de rang i de la borne K dans la base (β^{q-1}, ..., β^0) ($K_i = \sum_{j=0}^{q-1} (K_i)_j * \beta^j$ ou $K_i = (K_i)_{q-1} \ldots (K_i)_1 (K_i)_0$), j étant un indice de boucle, $(K_i)_j$ étant un nombre compris entre 0 et β-1 et q étant un degré du coefficient K_i,

E33_42 : on initialise à VRAI une deuxième variable booléenne g,

E33_43 : on réalise les opération suivantes, dans une boucle indicée par j variant entre q-1 et 0:

E33_431 : on produit une variable aléatoire $(S_i)_j$ comprise entre 0 et β-1,

E33_432 : si la variable aléatoire $(S_i)_j$ est strictement inférieure au coefficient $(K_i)_j$, alors on met à FAUX la deuxième variable booléenne g,

E33_4331 : si la variable aléatoire $(S_i)_j$ est strictement supérieure au coefficient $(K_i)_j$ et si la deuxième variable booléenne g est VRAI, alors on détermine un coefficient $(R_i)_j$ à partir de la variable aléatoire $(S_i)_j$ selon une fonction prédéfinie,

E33_4332 : sinon, poser $(R_i)_j = (S_i)_j$

E33_434 : on décrémente l'indice de boucle j,

E33_44 : on détermine le nombre aléatoire R_i par recombinaison des coefficients aléatoires $(R_i)_j$ dans la base β ($R_i = \sum_{j=0}^{q-1} (R_i)_j * \beta^j$ ou $R_i = (R_i)_{q-1} \ldots (R_i)_1 (R_i)_0$).

Comme on vient de le voir ci-dessus, en "imbriquant" deux procédés, on réduit le biais des nombres aléatoires R produits par le procédé global, tout en conservant un procédé global rapide. On peut bien sûr imaginer d"imbriquer" plus de deux procédés, par exemple trois ou quatre, en décomposant, dans l'étape E33_43 les nombres

dans une base $\gamma < \beta$, et en décomposant l'étape E33_43 en une succession d'étapes similaires aux étapes E33_41 à E33_43.

De manière générale, plus on "imbrique" de procédés, plus les nombres sur lesquels on travaille sont petits : la durée de chaque étape diminue et le biais des nombres produits par le procédé global diminue également.

L'invention a également pour objet un composant électronique adapté pour la mise en oeuvre d'un procédé tel que décrit ci-dessus. Un tel composant comprend notamment un générateur produisant des nombres aléatoires de taille N, et des circuits de calcul pour réaliser des opérations sur des nombres de au plus N bits.

Selon le mode de réalisation du procédé à mettre en œuvre, les circuits de calcul sont adaptés pour réaliser des opérations de comparaison de deux nombres, de troncature de nombre, de réduction modulaire.

Le générateur de nombres aléatoires et les circuits de calcul sont pilotés de préférence par un moyen logiciel mémorisé dans une mémoire du composant prévue à cet effet.

L'invention concerne également une carte à puce comprenant un composant électronique tel que décrit ci-dessus.

REVENDICATIONS

1. Procédé cryptographique, au cours duquel on utilise un générateur de nombres aléatoires produisant des nombres aléatoires S_i de taille N fixée compris entre 0 et W-1, pour produire un nombre aléatoire R compris entre 0 et une borne K prédéfinie, caractérisé en ce que :

E31 : on produit une variable aléatoire S_i comprise entre 0 et W-1,

E32 : si la variable aléatoire S_i est strictement inférieure à un coefficient K_i de la borne K dans la base W, alors le coefficient R_i de rang i du nombre aléatoire R est égal à la variable aléatoire S_i puis, pour tout rang j inférieur à i, on produit une variable aléatoire S_j entre 0 et W-1 et on pose $R_j = S_j$.

E33 : sinon, si la dite variable aléatoire est supérieure au coefficient K_i de rang i de la borne K dans la base W, alors on détermine le dit coefficient R_i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie, puis on détermine le coefficient R_{i-1} du nombre aléatoire R de rang i-1 immédiatement inférieur en répétant les étapes E31 à E33.

2. Procédé selon la revendication 1, au cours duquel on réalise les étapes suivantes :

E1 : on décompose la borne K dans une base $(W^0, W^1, \ldots, W^p)$ sous la forme $K = \sum_{i=0}^{p-1} K_i * W^i$, i étant un indice de boucle,

REVENDICATIONS

1. Procédé cryptographique, au cours duquel on utilise un générateur de nombres aléatoires produisant des nombres aléatoires S_i de taille N fixée compris entre 0 et W-1, pour produire un nombre aléatoire R compris entre 0 et une borne K prédéfinie, caractérisé en ce que :

E31 : on produit une variable aléatoire S_i comprise entre 0 et W-1,

E32 : si la variable aléatoire S_i est strictement inférieure à un coefficient K_i de la borne K dans la base W, alors le coefficient R_i de rang i du nombre aléatoire R est égal à la variable aléatoire S_i puis, pour tout rang j inférieur à i, on produit une variable aléatoire S_j entre 0 et W-1 et on pose $R_j = S_j$.

E33 : sinon, si la dite variable aléatoire est supérieure au coefficient K_i de rang i de la borne K dans la base W, alors on détermine le dit coefficient R_i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie, puis on détermine le coefficient R_{i-1} du nombre aléatoire R de rang i-1 immédiatement inférieur en répétant les étapes E31 à E33.

2. Procédé selon la revendication 1, au cours duquel on réalise les étapes suivantes :

E1 : on décompose la borne K dans une base (W^{p-1}, W^{p-2}, …, W^0) sous la forme $K = \sum_{i=0}^{p-1} K_i * W^i$, i étant un indice de

K_i étant un coefficient de la borne K de rang i compris entre 0 et W-1 et p étant le degré de la borne K,

E2 : on initialise à VRAI une variable booléenne f,

E3 : on réalise les opération suivantes, dans une boucle indicée par i, i étant un nombre entier variant entre p-1 et 0:

E31 : on produit une variable aléatoire S_i comprise entre 0 et W-1,

E32 : si la variable aléatoire S_i est strictement inférieure au coefficient K_i de rang i, alors on met à FAUX la variable booléenne f,

E33_1 : si la variable aléatoire S_i est strictement supérieure au coefficient K_i de rang i et si la variable booléenne f est VRAI, alors on détermine le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie,

E33_2 : sinon, on pose $R_i = S_i$

E34 : on décrémente la variable de boucle i,

E4 : on détermine le nombre aléatoire R par recombinaison des coefficients aléatoires R_i dans la base W selon la relation : $R = \sum_{i=0}^{p-1} R_i * W^i$.

3. Procédé selon la revendication 2, au cours duquel, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire Si de rang i (étapes E33_1 et E33_2), on réalise les sous-étapes suivantes :

E33_11: si la variable aléatoire S_i est strictement supérieure au coefficient K_i de la borne K, alors on produit une nouvelle variable aléatoire S_i,

boucle, K_i étant un coefficient de la borne K de rang i compris entre 0 et W-1 et p étant le degré de la borne K,

E2 : on initialise à VRAI une variable booléenne f,

E3 : on réalise les opération suivantes, dans une boucle indicée par i, i étant un nombre entier variant entre p-1 et 0:

E31 : on produit une variable aléatoire S_i comprise entre 0 et W-1,

E32 : si la variable aléatoire S_i est strictement inférieure au coefficient K_i de rang i, alors on met à FAUX la variable booléenne f,

E33_1 : si la variable aléatoire S_i est strictement supérieure au coefficient K_i de rang i et si la variable booléenne f est VRAI, alors on détermine le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie,

E33_2 : sinon, on pose $R_i = S_i$

E34 : on décrémente la variable de boucle i,

E4 : on détermine le nombre aléatoire R par recombinaison des coefficients aléatoires R_i dans la base W selon la relation : $R = \sum_{i=0}^{p-1} R_i * W^i$.

3. Procédé selon la revendication 2, au cours duquel, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire Si de rang i (étapes E33_1 et E33_2), on réalise les sous-étapes suivantes :

E33_11: si la variable aléatoire S_i est strictement supérieure au coefficient K_i de la borne K, alors on produit une nouvelle variable aléatoire S_i,

E33_12 : on répète l'étape E33_11 jusqu'à ce que la variable aléatoire S_i soit inférieure au coefficient K_i de la borne K, puis on égalise le coefficient R_i à la variable aléatoire S_i.

4. Procédé selon la revendication 2, au cours duquel, on choisit (étapes E33-1 et 33_2) le coefficient R_i de rang i égal à une partie de la variable aléatoire S_i, partie inférieure au coefficient K_i, la dite partie correspondant par exemple à un nombre limité de bits de la variable S_i.

5. Procédé selon la revendication 2, au cours duquel, au pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i (étape E33), on réduit la variable aléatoire S_i modulo K_i+1, le résultat de la réduction étant le coefficient R_i cherché.

6. Procédé selon l'une des revendications 1 à 5, au cours duquel, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire Si de rang i (étape E33), on exécute les étapes E1 à E4 en utilisant une base $(\beta^0, \beta^1, \ldots, \beta^q)$ comme base de calcul, β étant un nombre entier strictement inférieur à W et q étant le degré de K dans la base β.

7. Procédé selon la revendication 6, dans lequel l'étape E33 est décomposée en les sous-étapes suivantes :

E33_12 : on répète l'étape E33_11 jusqu'à ce que la variable aléatoire S_i soit inférieure au coefficient K_i de la borne K, puis on égalise le coefficient R_i à la variable aléatoire S_i.

4. Procédé selon la revendication 2, au cours duquel, on choisit (étapes E33-1 et 33_2) le coefficient R_i de rang i égal à une partie de la variable aléatoire S_i, partie inférieure au coefficient K_i, la dite partie correspondant par exemple à un nombre limité de bits de la variable S_i.

5. Procédé selon la revendication 2, au cours duquel, au pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i (étape E33), on réduit la variable aléatoire S_i modulo K_i+1, le résultat de la réduction étant le coefficient R_i cherché.

6. Procédé selon l'une des revendications 1 à 5, au cours duquel, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire Si de rang i (étape E33), on exécute les étapes E1 à E4 en utilisant une base $(\beta^{q-1}, \ldots, \beta^0)$ comme base de calcul, β étant un nombre entier strictement inférieur à W et q étant le degré de K dans la base β.

7. Procédé selon la revendication 6, dans lequel l'étape E33 est décomposée en les sous-étapes suivantes :

E33_41 : on décompose le coefficient K_i de rang i de la borne K dans la base (β^0, β^1, ..., β^p) sous la forme $K_i = \sum_{j=0}^{q-1} (K_i)_j * \beta^j$, j étant un indice de boucle, $(K_i)_j$ étant un nombre compris entre 0 et β-1 et q étant le degré du coefficient K_i,

E33_42 : on initialise à VRAI une deuxième variable booléenne g,

E33_43 : on réalise les opération suivantes, dans une boucle indicée par j variant entre q-1 et 0:

E33_431 : on produit une variable aléatoire $(S_i)_j$ comprise entre 0 et β,

E33_432 : si la variable aléatoire $(S_i)_j$ est strictement inférieure au coefficient $(K_i)_j$, alors on met à FAUX la deuxième variable booléenne g,

E33_4331 : si la variable aléatoire $(S_i)_j$ est strictement supérieure au coefficient $(K_i)_j$ et si la deuxième variable booléenne g est VRAI, alors on détermine un coefficient $(R_i)_j$ à partir de la variable aléatoire $(S_i)_j$ selon une fonction prédéfinie,

E33_4332 : sinon, poser $(R_i)_j = (S_i)_j$

E33_434 : on décrémente l'indice de boucle j,

E33_44 : on détermine le nombre aléatoire R_i par recombinaison des coefficients aléatoires $(R_i)_j$ dans la base β selon la relation : $R_i = \sum_{j=0}^{q-1} (R_i)_j * \beta^j$.

8. Composant électronique comprenant un générateur de nombres aléatoires de taille N, des circuits de calcul réalisant notamment une comparaison, une troncature et / ou une réduction modulaire sur des nombres de au plus N bits, et un moyen de pilotage du générateur de nombres aléatoires et des circuits de calcul, le dit moyen de

E33_41 : on décompose le coefficient K_i de rang i de la borne K dans la base (β^{q-1}, ..., β^0) sous la forme $K_i = \sum_{j=0}^{q-1} (K_i)_j * \beta^j$, j étant un indice de boucle, $(K_i)_j$ étant un nombre compris entre 0 et β-1 et q étant le degré du coefficient K_i,

E33_42 : on initialise à VRAI une deuxième variable booléenne g,

E33_43 : on réalise les opération suivantes, dans une boucle indicée par j variant entre q-1 et 0:

E33_431 : on produit une variable aléatoire $(S_i)_j$ comprise entre 0 et β - 1,

E33_432 : si la variable aléatoire $(S_i)_j$ est strictement inférieure au coefficient $(K_i)_j$, alors on met à FAUX la deuxième variable booléenne g,

E33_4331 : si la variable aléatoire $(S_i)_j$ est strictement supérieure au coefficient $(K_i)_j$ et si la deuxième variable booléenne g est VRAI, alors on détermine un coefficient $(R_i)_j$ à partir de la variable aléatoire $(S_i)_j$ selon une fonction prédéfinie,

E33_4332 : sinon, poser $(R_i)_j = (S_i)_j$

E33_434 : on décrémente l'indice de boucle j,

E33_44 : on détermine le nombre aléatoire R_i par recombinaison des coefficients aléatoires $(R_i)_j$ dans la base β selon la relation : $R_i = \sum_{j=0}^{q-1} (R_i)_j * \beta^j$.

8. Composant électronique comprenant un générateur de nombres aléatoires de taille N, des circuits de calcul réalisant notamment une comparaison, une troncature et / ou une réduction modulaire sur des nombres de au plus N bits, et un moyen de pilotage du générateur de nombres aléatoires et des circuits de calcul, le dit moyen de

pilotage étant adapté pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 7.

9. Carte à puce comprenant un composant électronique selon la revendication précédente.

pilotage étant adapté pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 7.

9. Carte à puce comprenant un composant électronique selon la revendication précédente.

reçue le 28/01/04

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

INV

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier *(facultatif)*	0312435
N° D'ENREGISTREMENT NATIONAL	016916

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé et dispositif associé de génération de nombres aléatoires dans un intervalle donné.

LE(S) DEMANDEUR(S) :

GEMPLUS
Avenue du Pic de Bertagne
Parc d'activités de Gemenos
13420 GEMENOS
FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		JOYE
Prénoms		Marc
Adresse	Rue	19, rue Voltaire
	Code postal et ville	8 3 6 4 0 SAINT ZACHARIE
Société d'appartenance *(facultatif)*		
2 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Jean-Louis LECLAIRE - 93.4009

CABINET BALLOT
CONSEILS EN PROPRIÉTÉ INDUSTRIELLE
9, rue Claude Chappe
Technopôle Metz 2000
57070 METZ

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.